SPECIAL EDITION

CYBER SECURITY AND YOU

July 14, 2000

CIO Update

United States Department of Energy

Special Edition 1

The "ILoveYou" Virus

Computer viruses make headline news when a new and innovative approach unleashes a new strain. The *ILoveYou* and its variation the *NewLove* viruses are the latest ones that got past our defenses. Each new variation seems to spread more quickly and have more impact. There will be others that will also elude our defenses. What can **YOU** do to thwart a virus all together?

Most viruses have one thing in common - they need **YOUR** involvement in some manner to execute. Although there are some exceptions, nearly all viruses need to be manually activated by **YOU** in some fashion. This means **YOU** have to do something over and above just opening the e-mail. **YOU** must do something with the attachments. This may not always be as obvious as double clicking on an attached executable file. Many viruses hide themselves as macros within documents. **YOU** double click on the attached document and **YOU** are not only opening the document but are executing any macros within that document. **YOU** may not realize **YOU** are running a program but that macro is a program.

Here are some things **YOU** should do:

The most important rule is to be knowledgeable of how most viruses work as described above. The second most important rule is to be knowledgeable of **YOUR** normal day-to-day operating situation. Armed with this knowledge **YOU** will be on the lookout for unexpected strange e-mail messages and their attachments. Before opening an e-mail, **YOU** should perform this mental checklist:

1. ***Is it from someone I know?*** If not, do not open it.
2. ***If it is from someone I know,*** was I expecting an e-mail and this particular attachment? Is the name of the attachment out of the ordinary? Confirm with the sender.
3. ***What type of file is the attachment?*** If it appears to be an executable program (with an extension of .EXE, .COM, or .VBS, for instance), be especially suspicious. Confirm with the sender.
4. ***When you finally open the file, do any alerts or warnings display?*** If this is unexpected confirm with the sender.

These are a few steps **YOU** can take in **YOUR** day to day work to reduce the potential for viruses to affect **YOU.**

How You Can Help in the Fight Against Computer Viruses

The 8-day global rampage of the *ILoveYou* virus, believed to have been created by amateur saboteurs in the Philippines, is estimated to have cost $8 billion in lost productivity, data, and opportunity. Numerous DOE sites and organizations were disrupted. With new viruses constantly being unleashed and becoming more subtle in their attack methods, the daily email correspondence we take for granted has an element of threat. The best approach may be to meet this threat by actively taking steps, such as the ones below, to secure your desktop computer against computer viruses.

Make sure your system is protected by anti-virus software that is up to date. Ultimately, this is the best and most essential protection. And remember, simply installing anti-virus software is not enough; you have to keep it up to date with the latest virus signatures, which are released almost daily. At work, installation and updates should occur automatically. Check with your computer support staff for information.

Activate any warning mechanisms you can that may alert you to a possible problem. For instance, make sure the warning that a macro exists in a document is turned on in Microsoft Word. If the warning is displayed and you don't think the document should have macros, there may be a virus, and you should disable it. If you need assistance, contact your computer support staff.

If you think your computer has been infected with a virus, contact your computer support staff immediately. Viruses can do a wide variety of damage, and, once your system is infected, simply deleting or clearing the infected files or programs may not be sufficient. Let someone who knows all of the ramifications help you.

These are a few steps you can take in your day-to-day work to reduce the potential for dangerous viruses affecting DOE and you. The keys are to be aware

of how viruses spread, know YOUR normal work process, and remember to consider viruses before acting. No matter how enticing a message may be ("I love you" can be a powerful motivator), be skeptical. When interacting with e-mail attachments, assume an attachment has a virus infection and act on that premise. Only when you are absolutely sure the attachment is valid should you open it. ***When in doubt, keep it out.***

Cyber Threats

Cyber threats take many forms. **Intelligence collectors,** who may be foreign intelligence agents, seek information for economic advantage or insight into national security issues. They may be from adversarial or friendly nations. **Terrorists** usually are individuals motivated by a deeply held grievance, religious zeal, or perceived injustice. They gather information to support their activities or to plan attacks. **Hackers** may be youths motivated by the thrill, experienced hackers motivated by philosophical ideals, professionals hired by foreign governments, or criminals motivated by the promise of quick and easy money.

Most insidious is the threat from insiders. **Traitors** collect information and provide it to an adversary. **Disgruntled employees** may intentionally destroy, damage, or disrupt computer systems. **Browsers** may access or attempt to access information they have no need to know, such as another employee's personnel information. **Incompetent people** may, through ignorance, corrupt or destroy system files. **Others** may inadvertently cause damages or system disruptions by not paying attention to what they are doing, or because they lack knowledge and training. Being aware that these threats exist and taking them seriously is the first step toward security awareness in the workplace.

Crosstalks Cover Cutting Issues

Cyber security issues are many and varied with crosscutting, Departmentwide implications. Knowing the issues and having expert recommendations makes for a more cyber-secure environment. The Office of Security and Emergency Operations offers Crosstalk papers that describe a variety of cyber security issues, such as DOE web server compromises, laptop security concerns, incident reporting, and password policy. Crosstalks provide lessons learned and make specific recommendations. Access Crosstalks at http://www.so.doe.gov/crostk_f.htm.

CIAC Automates Break-in Detection, Prevention

The Computer Incident Advisory Capability (CIAC), based at the Lawrence Livermore National Laboratory, is in the early stages of developing a firewall or router log analysis service for DOE facilities. This service can help sites fend off cyber attacks. When fully operational, CIAC will provide each participating site with a process for automating and protecting the transmission of the data in their daily log files. CIAC will then analyze the data to detect a variety of suspicious activities and patterns.

The analysis of firewall or router logs can be one component of building an effective defense against cyber break-ins. CIAC finds that a careful analysis of firewall logs can have a significant value in detecting activities that may precede an attempted cyber break-in. Many times, when a break-in has been reported to CIAC, a check of prior logs reveals a pattern of attempts which have preceded the actual break-in. CIAC has found that a cyber adversary frequently has attacked multiple DOE sites. Detecting the adversary during the exploratory phase allows time to prepare a defense to thwart a full-fledged break-in.

By examining log files from a large number of sites, CIAC's automated methodology has the potential to establish patterns of intrusion making it possible to predict patterns of attack. By automating these processes, log analysis can establish the fact of an adversarial scan and automatically report that fact to all other sites so that they can take preventative measures. CIAC's new approach encapsulates that group's experience with reviewing log files into an automated process that will allow CIAC to cost effectively multiply its effort across a large number of sites.

CIAC's analysis will compare information from the logs of other sites and from other sources such as the "CIAC Bad List" that lists IP (Internet Protocol) addresses that previously have been reported to CIAC as having launched attacks against DOE facilities. Other analyses will correlate attempted intrusions at one site to the same activity at another site. When the analysis is complete, CIAC's automated process will generate and email a report to the reporting site. Each participating site will have a limited capability to tailor the content of CIAC's report.

CIAC plays a key role in DOE's cyber security program. CIAC bulletins, advisories, security tools, and specialized security information resources are available on the CIAC web site (http://ciac.llnl.gov). As this analysis service begins to be deployed, more information will be made available on the DOE Secure Server at https://doesecure.ciac.org/. CIAC's 24-hour hot-line is available to help with computer security incidents (telephone: 925-422-8193; email ciac@ciac.org).